

ICS 33.050

CCS M 30

团体标准

T/TAF 078.6—2023
代替 T/TAF 078.6—2020

APP 用户权益保护测评规范 第 6 部分：违规收集个人信息

Application software user rights protection evaluation specification—
Part 6: Illegal collection of personal information

2023-06-26 发布

2023-06-26 实施

电信终端产业协会 发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 违规收集个人信息	3
5.1 概述	3
5.2 未见明示	3
5.3 有明示未同意	3
5.4 明示不清晰	3
5.5 未见明示 SDK	3
5.6 明示 SDK 未同意	4
5.7 明示 SDK 不清晰	4
5.8 同意不清晰	4
5.9 默认同意	4
5.10 拒绝同意	4
参考文献	5

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是T/TAF 078《APP用户权益保护测评规范》的第6部分。T/TAF 078 已发布了以下部分：

- 第1部分：超范围收集个人信息；
- 第2部分：定向推送；
- 第3部分：个人信息获取行为；
- 第4部分：权限索取行为；
- 第5部分：违规使用个人信息；
- 第6部分：违规收集个人信息；
- 第7部分：欺骗误导强迫行为；
- 第8部分：移动应用分发平台管理；
- 第9部分：移动应用分发平台信息展示；
- 第10部分：自启动和关联启动行为。

本文件代替T/TAF 078.6—2020《APP用户权益保护测评规范 违规收集个人信息》，与T/TAF 078.6—2020相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 题目增加了“第6部分：”；
- b) 增加了规范引用文件（见第2章）；
- c) 增加了“用户”“同意”等的定义（见第3章）；
- d) 增加概述（见5.1）；
- e) 增加突出显示敏感个人信息的内容（见5.2 b)、5.5 b)）；
- f) 增加默认同意的内容（见5.9 b)）；
- g) 增加拒绝同意的要求（见5.10）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、泰尔认证中心有限公司、蚂蚁科技集团股份有限公司、武汉安天信息技术有限责任公司、维沃移动通信有限公司、OPPO广东移动通信有限公司。

本文件主要起草人：陈鑫爰、周飞、李可心、李京典、王艳红、杜云、宁华、臧磊、常浩伦、李鑫、赵昕、林冠辰、陈诚、余丽娜、张玮、李腾、赵鹏阳。

本文件及其所代替文件的历次版本发布情况为：

- 2020年首次发布为T/TAF 078.6—2020；
- 本次为第一次修订。

引 言

本文件根据《中华人民共和国网络安全法》等相关法律要求，依据《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》《关于进一步提升移动互联网应用服务能力的通知》提出检测细则，进一步促进移动互联网行业的健康稳定发展。



APP 用户权益保护测评规范 第 6 部分：违规收集个人信息

1 范围

本文件规定了移动应用软件及第三方软件开发工具包违规收集个人信息部分的检测细则以及典型检测场景。

本文件适用于移动应用软件提供者规范用户收集使用个人信息处理活动，也适用于主管部门、第三方评估机构等组织对移动应用软件收集使用个人信息行为进行监督、管理和评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 41391—2022 信息安全技术 移动互联网应用程序 (App) 收集个人信息基本要求

YD/T 2407—2021 移动智能终端安全能力技术要求

YD/T 4177.1—2022 移动互联网应用程序 (APP) 收集使用个人信息最小必要评估规范 第 1 部分：总则

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动智能终端 smart mobile terminal

能够接入移动通信网，具有能够提供应用软件开发接口的操作系统，具有安装、加载和运行应用软件能力的终端。

[来源：YD/T 2407—2021，3.1.1]

3.2

移动互联网应用程序 mobile Internet application

可安装在移动智能终端内，能够利用移动智能终端操作系统提供的公开开发接口，实现某项或某几项特定任务的应用程序。

注：包含移动智能终端预置应用、小程序、快应用以及互联网信息服务提供者提供的可以通过网站、应用商店等应用分发平台下载、安装、升级的应用程序，简称 App。

3.3

收集 collect

获得个人信息的活动。

[来源：YD/T 4177.1—2022, 3.7]

3.4

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。

[来源：《中华人民共和国个人信息保护法》]

3.5

敏感个人信息 sensitive personal information

一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。

[来源：《中华人民共和国个人信息保护法》]

3.6

用户 user

使用产品或服务的个人信息主体。

[来源：GB/T 25069—2022, 3.733, 有修改]

3.7

同意 consent

个人信息主体对其个人信息进行处理自愿、明确作出授权的行为。

注：包括通过积极的行为作出授权（即明示同意），或者通过个人信息主体的行为而推定其作出授权。

3.8

软件开发工具包 software development kit

协助软件开发的软件库。

注：软件工具开发包简称 SDK, 通常包括相关二进制文件、文档、范例和工具的集合。

[来源：GB/T 41391—2022, 3.14, 有修改]

4 缩略语

下列缩略语适用于本文件。

IMEI: 国际移动设备识别码 (International Mobile Equipment Identity)

IMSI: 国际移动用户识别码 (International Mobile Subscriber Identity)

MAC: 媒体存取控制 (Media Access Control)
 IDFA: 广告标识符 (Identifier For Advertising)
 IDFV: 供应商标识符 (Identifier For Vendor)
 OAID: 匿名设备标识符 (Open Anonymous Device Identifier)
 MEID: 移动设备识别码 (Mobile Equipment Identifier)
 ICCID: 集成电路卡识别码 (Integrate Circuit Card Identity)
 SN: 设备序列号 (Serial Number)
 SUCI: 用户隐藏标识符 (Subscription Concealed Identifier)
 SUPI: 用户永久标识符 (Subscription Permanent Identifier)

5 违规收集个人信息

5.1 概述

违规收集个人信息的行为包括未见明示、有明示未同意、明示不清晰、未见明示SDK、明示SDK未同意、明示SDK不清晰、同意不清晰、默认同意和拒绝同意, 出现上述任意一种行为, 则判定为违规收集个人信息。

5.2 未见明示

未见明示具体场景包括但不限于:

- a) APP 未以个人信息处理规则弹窗等形式向用户明示个人信息处理的目的、方式和范围, 收集IMEI、IMSI、设备MAC地址、Android ID、OAID、IDFA、IDFV、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息;
- b) APP 个人信息处理规则中未以字体加粗、增大字号、醒目颜色等方式突出展示APP处理个人敏感信息的目的、方式和范围。

5.3 有明示未同意

APP 以个人信息处理规则弹窗等形式向用户明示个人信息处理的目的、方式和范围, 未经用户同意, 收集IMEI、IMSI、设备MAC地址、Android ID、OAID、IDFA、IDFV、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息。

5.4 明示不清晰

APP 以个人信息处理规则弹窗等形式向用户明示个人信息处理的目的、方式和范围, 未清晰明示处理IMEI、IMSI、设备MAC地址、Android ID、OAID、IDFA、IDFV、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息的目的、方式和范围, 用户同意后, 收集相应个人信息; 未清晰明示在静默状态下或在后台运行时收集个人信息的目的、方式和范围, 收集相应个人信息。

5.5 未见明示 SDK

未见明示 SDK 具体场景包括但不限于:

- a) APP 未以个人信息处理规则弹窗等形式向用户明示第三方 SDK 处理个人信息的目的、方式和

范围，第三方 SDK 不应收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、IDFA、IDFV、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息；

- b) APP 个人信息处理规则中未以字体加粗、增大字号、醒目颜色等方式突出展示或标识第三方 SDK 处理个人敏感信息的目的、方式和范围。

5.6 明示 SDK 未同意

APP 以个人信息处理规则弹窗等形式向用户明示第三方 SDK 处理个人信息的目的、方式和范围，未经用户同意，第三方 SDK 收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、IDFA、IDFV、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息。

5.7 明示 SDK 不清晰

APP 以个人信息处理规则弹窗等形式向用户明示第三方 SDK 处理个人信息的目的、方式和范围，未清晰明示第三方 SDK 处理 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、IDFA、IDFV、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息的目的、方式和范围，用户同意后，第三方 SDK 收集相应个人信息；未清晰明示在静默状态下或在后台运行时第三方 SDK 收集个人信息的目的、方式和范围，第三方 SDK 收集相应个人信息。

注：5.5、5.6、5.7 节中 APP 通过技术手段或从 SDK 获得等方式向用户明示可获知的 SDK 处理的个人信息的目的、方式和范围。从 SDK 获得的方式中，SDK 有义务向 APP 告知所处理的个人信息的目的、方式和范围及变化情况。

5.8 同意不清晰

APP 在征求用户同意环节，未提供明确的同意和拒绝选项，仅使用“好的”、“我知道了”等无法清晰表达用户同意的词语。

5.9 默认同意

默认同意具体场景包括但不限于：

- a) APP 在征求用户同意环节，设置为默认同意；
- b) APP 收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户并征得用户再次同意。

5.10 拒绝同意

用户拒绝提供非当前服务所必需的个人信息时，APP 拒绝用户使用该服务的基本功能。

参 考 文 献

- [1] 中华人民共和国个人信息保护法



电信终端产业协会团体标准

APP 用户权益保护测评规范 第 6 部分：违规收集个人信息

T/TAF 078.6—2023

*

版权所有 侵权必究

电信终端产业协会印发

地址：北京市西城区新街口外大街 28 号

电话：010-82052809

电子版发行网址：www.taf.org.cn